

Remarks

In the present application, claims 1, 2, 3, 11, 14, 15, 17, 18, 19, 20, and 23 to 25 have been amended. New claim 26 has been added, including features claimed in claims 1 and 3. Amendments to the Specification including a new Title and a new Abstract have been submitted. Reexamination and reconsideration of the present application in view of these amendments and the following remarks is respectfully requested.

Objections to the Specification

The Examiner objected to the Abstract for exceeding 150 words. A new Abstract of less than 150 words has been submitted and withdrawal of the objection to the Specification is requested.

Objections to the Specification

The Examiner objected to claim 3 for having a misspelled word. Claim 3 has been amended to correct the spelling and withdrawal of the objection is requested.

Claim Rejections for Anticipation

The Examiner rejected claims 1 to 4 and 6 to 13 under 35 U.S.C. §102(e) as anticipated by Wilson, et al., U.S. Patent No. 6,047,281. These rejections are respectfully traversed.

Claim 1, as amended, recites in part a method of verifying the identity of a registered user selected from a group consisting of persons and entities. The method includes obtaining a list of at least two identity verifiers, with each identity verifier to be used for no more than one transaction. The identity verifiers on the list are linked to at least one unique numerical identifier associated with the registered user. A numerical identifier and an identity verifier are received from a requesting party. It is determined if the received identity verifier is within the list of identity verifiers linked to the received numerical identifier. This determination is communicated to the requesting party.

In Wilson, the method disclosed relates to finding an identity based on the analysis of one or more biometric data, such as fingerprints. Wilson does not disclose

using a known identity and known identity verification data, and verifying that the identity verification data are linked to the identity.

Wilson does not disclose that non-biometric data be included in the identity search and verification process, and thus, Wilson is limited to finding the identity of persons only. Claim 1 recites that the group of registered users whose identity may be verified includes both persons and entities. Entities, as used in the Specification, may be any party with whom a person may be dealing. These parties may be individuals or may be legal entities, such as an on-line retailer. Wilson discloses that other types of data than fingerprints may be used, but only discloses such alternatives be items which are used to identify and verify the identity of a person, such as other biometric data.

Further, Wilson does not disclose that the identity verifiers, i.e., the biometric data, be used for only one transaction. There is no disclosure in Wilson where an identification verifying element, such as a particular biometric data regarding a person, be intended for use in only a single identity verification process. In fact, Wilson, at col. 8, lines 38 to 58, suggests that the biometric data can be used multiple times for multiple purposes, such as authenticating financial transactions, drivers licenses, insurance claims, voter registration, medical orders, etc. Thus, if a person is able to replicate the biometric data of another, the same verification data can be used over and over. Claim 1 recites that an identity verifier be valid for only a single use.

For at least these reasons, Applicant submits that Wilson does not anticipate claim 1 and that claim 1 is in condition for immediate allowance. Claims 2 to 5 and 6 to 13 depend from and further limit claim 1.

With respect to claim 2, the Examiner referenced col. 7, lines 11 to 49, as disclosing that a transaction verification identifier be communicated to the requesting party to indicate if the identity verifiers was within the list of identity verifiers linked to the numerical identifier. Applicant finds no such disclosure within the prior art and respectfully requests the Examiner point out more precisely those elements of the cited prior art which disclose use of a transaction verification identifier as recited in claim 2.

With respect to claim 3, the Examiner referenced col. 8, lines 23 to 37, as disclosing the step of communicating a signal to the requesting party that the identity

verifier has been used before. Applicant cannot find a disclosure of this nature at this location, or elsewhere in the cited prior art.

With respect to claim 4, the Examiner referenced col. 9, lines 10 to 24 as disclosing the step of archiving the identity verifier and the verification transaction identifier. Applicant cannot find a disclosure of this nature at this location, or elsewhere in the cited prior art.

With respect to claim 11, the Examiner referenced col. 12, lines 25 to 57, as disclosing that the determining step includes determining whether the received identity verifier is linked to the received numerical identifier and the received uniqueness suffix. Applicant submits that no such uniqueness suffix is disclosed in the cited prior art. There is not disclosure in Wilson that the subject identifiers require or might include any uniqueness index to make the number unique. Indeed, Wilson discloses that these identity verifiers are unique and as such there is no need for any additional uniqueness suffix, as recited in claim 11.

With respect to claim 12, the Examiner referenced col. 6, lines 44 to 53, as disclosing the step of receiving a numerical identifier, receiving an identity verifier, and communicating information to the requesting party by voice communication over a phone line. However, Wilson discloses only that event messages and alert messages from all application tasks be captured via modem by a log manager. There is no disclosure that the requesting party communicate by voice the information to be verified over a phone line or that information be communicated by voice to the requesting party over a phone line.

For at least these reasons and those cited above with regard to claim 1, Applicant submits that claims 2 to 4 and 6 to 13 are not anticipated by the cited prior art and that claims 2 to 4 and 6 to 13 are in condition for immediate allowance.

Reexamination and reconsideration are respectfully requested.

Claims 14, 17 to 19, 23 and 24 were rejected under 35 U.S.C. §102(e) as anticipated by Pare, Jr., et al., U.S. Patent No. 6,154,879. These rejections are respectfully traversed.

Claim 14, as amended, recites in part a method of determining whether an identity verifier is required to be submitted in a particular transaction. The method includes the steps of obtaining a list of identity verifiers, each identity verifier to be used for no more than one transaction. The identity verifiers are linked to at least one unique numerical identifier associated with a registered user who may be selected from a group consisting of persons and entities. Categories of transactions are created. The registered user provides instructions designating categories of transactions requiring an identity verifier. The numerical identifier is received from a requesting party along with information regarding the type of transaction occurring. It is determined if the desired transaction is within a category requiring an identity verifier. Information is communicated to the requesting party indicating whether an identity verifier is required.

Pare discloses a tokenless biometric access system for accessing financial accounts through an ATM. While Pare does disclose linking a list of identity verifiers to a numerical identifier associated with a registered user, it does not disclose that the identity verifier is intended to be used only one time. In fact, it is clear from the reference that the identity verifier is intended to be used multiple times as a substitute for having to carry and insert an ATM card to initiate and carry out transactions at an ATM. Pare does not disclose creating categories of transactions and segregating categories of transaction requiring identity verification from categories not requiring identity verifiers. Further, Pare does not disclose any category of transaction which does not require the identity verification. In fact, the only method of initiating a transaction disclosed in Pare is to provide an identity verifier in the form of a biometric characteristic.

Further, Pare only discloses a system for verifying the identity of an individual through the use of biometric data and characteristics. For a user which is an entity, such as an on-line retailer, no such biometric data would be available.

For at least these reasons, Applicant submits that claim 14 is not anticipated by the cited prior art and that claim 14 is in condition for immediate allowance. Reexamination and reconsideration are respectfully requested.

Claims 17 to 19 have been amended to depend from claim 15. Claims 23 and 24 have been amended to depend from claim 20. As such, Applicant submits that these

rejections of claims 17 to 19, 23 and 24 have been overcome. A discussion of the rejection of claims 15 and 20 follows in the remarks below.

The Examiner rejected claims 15 and 16 under 35 U.S.C. §102(e) as anticipated by Challenger, et al., U.S. Patent No. 6,081,793. These rejections are respectfully traversed.

Claim 15, as amended, recites in part an identity verification system for verifying the identity of a registered user selected from a group of persons and entities. The system includes a database configured to receive at least one unique numerical identifier associated with the registered user and at least two identification verifiers associated with the registered user. The identification verifiers are to be used for no more than one transaction. The system also includes an input module for inputting the numerical identifier and the identification verifiers so that they are linked in the database. A communications module receives a numerical identifier and an identification verifier from a requesting party and communicates to the requesting party if the two are linked in the database. A processor module compares the received identifiers to the database to determine if they are linked and if the identification verifier has been used before.

In Challenger, the system discloses only that a single identification verifier, the PIN, be stored and associated with a voter's ID. There is no disclosure of a second or any additional identification verifiers associated with the smart card. Also, while the PIN is disclosed as included on the smart card, the PIN is not disclosed as included within a database associated with the voter ID. If the PIN input by the person using the smart card is the same as that embedded on the smart card, the transaction, voting, is allowed to proceed. Challenger does not disclose that new smart cards and/or new PINs are to be issued each time an election is organized, so that there is no disclosure that the PIN is intended for use only a single transaction.

For at least these reasons, Applicant submits that the cited prior does not anticipate claim 15, and that claim 15 is in condition for immediate allowance. Reexamination and reconsideration is respectfully requested.

As noted above, claims 17 to 19 depend from and further limit claim 15. For at least the same reasons cited above with regard to claim 15, Applicant submits that claims

17 to 19 are also in condition for immediate allowance. Reexamination and reconsideration are respectfully requested.

The Examiner rejected claims 20 to 22 under 35 U.S.C. §102(b) as anticipated by Kaehler, et al., U.S. Patent No. 4,967,366. These rejections are respectfully traversed.

Claim 20, as amended, recites in part a remote terminal for communicating with an identity verification system including an input module, a communications module and an output module. The input module is for inputting a numerical identifier and an identification verifier. The communications module sends the input information to a remotely located system storing a plurality of numerical identifiers and identification verifiers linked with the numerical identifiers. The communications module also receives a message from the remote system indicating if the input numerical identifier is linked with the input identification verifier, and whether the identification verifier has been used before. The communications module also receives a verification transaction identifier and a security message linked to the identification verifier. The output module reports the messages received by the communications module. The remote system stores numerical identifiers which are associated with registered users selected from a group consisting of persons and entities.

Kaehler discloses a gasoline dispenser and point of sale authorization system. The system of Kaehler is intended to permit a user to input privately a commonly used PIN. This same PIN is used for multiple transactions with the credit card number. There is no disclosure in Kaehler that any message be returned to the PIN pad or to the dispenser head regarding whether or not the PIN had been used before. There is no disclosure in Kaehler that multiple PINs be provided for a given credit card number.

For at least these reasons, Applicant submits that Kaehler does not anticipate claim 20 and that claim 20 is in condition for immediate allowance. Claims 21 to 24 depend from and further limit claim 20. For at least the same reasons cited above with regard to claim 20, Applicant submits that claims 21 to 24 are not anticipated by the cited prior art and that claims 21 to 24 are in condition for immediate allowance. Reexamination and reconsideration are respectfully requested.

The Examiner rejected claim 25 under 35 U.S.C. §102(e) as anticipated by Kuhns, et al., U.S. Patent No. 5,553,155. This rejection is respectfully traversed.

Claim 25, as amended, recites in part a computer program storage medium encoding a computer program of instructions for verifying the identity of a registered user. The program includes storing at least two identity verifiers in a database, each verifier to be used for no more than one transaction. At least one numerical identifier associated with the registered user is also stored in the database and the verifiers are linked with one of the numerical identifiers. A numerical identifier and an identity verifier are received. The received information is compared with the stored information to determine whether the received identity verifier is one of the verifiers linked with the numerical identifier in the database. The program also communicates information as to whether the received identity verifier is one of the identity verifiers linked to the numerical identifier in the database, and whether the identity verifier has been used before.

Kuhns discloses a method for thwarting fraud in the issuance of food stamps or other government entitlement programs. Kuhns discloses that a benefit recipient receives a card on which is coded a PIN. A biometric index for the recipient is generated based on biometric data regarding the recipient. The biometric index is used to assign the recipient a time slot for redeeming benefits using the card. When the recipient attempts to redeem the benefits using the card, the PIN is read from the card and used to retrieve the recipient's biometric index. If the card is being presented within the assigned time slot, the benefits are released to the recipient. (See col. 3 line 50 to col. 4, line 51). The same card is to be used for multiple months, and thus for multiple redemption transactions. The biometric index may also be used multiple times in conjunction with the PIN.

Alternatively, Kuhns discloses that a particular biometric identifier, such as a person's face, may be used to verify the identity of the person presenting the card to redeem benefits. Such a biometric identifier may be pulled from the database or printed directly on the front of the card.

Kuhns does not disclose that an identity verifier be used a single time. Ideally, to avoid fraud, the same biometric data, such as the face, is used each time the card is presented to redeem benefits. In this way, the benefit granting agency can have some

certainty that the person to whom the card was issued is the person presenting the card for benefits. Kuhns also does not disclose that information regarding whether the identity verifier has been used is communicated by the system or even collected by the system.

For at least these reasons, Applicant submits that the cited prior art does not anticipate claim 25 and that claim 25 is in condition for immediate allowance. Reexamination and reconsideration are respectfully requested.

Claim 5 was rejected under 35 U.S.C. §103(a) as obvious over Wilson, et al., U.S. Patent No. 6,047,281, as applied to claim 1, in view of Kuhns, et al., U.S. Patent No. 5,224,173. This rejection is respectfully traversed.

Claim 5 depends from and further limits claim 1. Claim 5 recites in part that the method further includes storing public information regarding the registered user and creating at least two categories of requesting parties. The registered user provides instructions as to what public information may be released to each of the different categories of requesting parties. Based on the category of requesting user, the appropriate public information is communicated to the requesting party.

Wilson is cited as providing the features of claim 1, from which claim 5 depends, and Kuhns is cited as providing the features of claim 5. As discussed above, Applicant submits that Wilson does not disclose the features of the method recited in claim 1. Further, there is no teaching or suggestion within Wilson that would lead a person of ordinary skill in the art to modify Wilson in such a manner as to render claim 1 obvious. As noted above, Wilson actually teaches away from the features of claim 1, in that use of biometric data precludes inclusion of entities in the list of registered users. Wilson also does not teach or suggest the use of any identity verifier for no more than one transaction.


The Examiner noted that Wilson does not teach various elements recited in claim 5. Kuhns is not cited as providing any of the features of claim 1. Kuhns does not teach or suggest that the registered user provide instructions regarding which public information is to be communicated to a requested party based on the category of transaction in which identity verification is requested.

For at least these reasons, Applicant submits that claim 5 is not rendered obvious by the cited prior art and that claim 5 is in condition for immediate allowance. Reexamination and reconsideration are respectfully requested.

If the Examiner has any questions regarding this Amendment and Response, the Examiner is invited to contact Applicant's representative Alan Stewart at 612.371.5376.

Respectfully submitted,
MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(612) 332-5300

Date: August 20, 2004

By: 
Name: Alan R. Stewart
Reg. No.: 47,974
ARS:pll